1. What is a cybersecurity vulnerability?

A **cybersecurity vulnerability** is a weakness or flaw in a system, network, application, or process that could be exploited by a threat actor to gain unauthorized access, disrupt operations, steal data, or otherwise compromise the integrity, confidentiality, or availability of an asset.

Key Aspects:

1. **Types of Vulnerabilities:**
   - **Software Vulnerabilities:** Bugs or misconfigurations in software, such as outdated libraries, unpatched systems, or buffer overflows.
   - **Hardware Vulnerabilities:** Issues in physical components, like Spectre and Meltdown in CPUs.
   - **Human Vulnerabilities:** Social engineering exploits human error, such as phishing or weak password usage.
2. **Common Examples:**
   - Missing patches or updates.
   - Misconfigured firewalls or access controls.
   - Weak encryption protocols.
   - Insecure APIs.
3. **Lifecycle:**
   - **Discovery:** Identified by researchers, attackers, or users.
   - **Disclosure:** Reported to vendors or made public.
   - **Exploitation:** Threat actors take advantage of the flaw.
   - **Remediation:** Patches or mitigation strategies are implemented.
4. **Famous Vulnerabilities:**
   - **Heartbleed (2014):** A flaw in OpenSSL that allowed data theft from encrypted connections.
   - **Log4Shell (2021):** A vulnerability in Log4j that enabled remote code execution.
5. **Vulnerability Management:**
   - **Identify:** Use tools like vulnerability scanners.
   - **Assess:** Determine the risk level.
   - **Remediate:** Apply patches or mitigations.
   - **Monitor:** Regularly review and reassess.